UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,803	08/09/2006	Wataru Matsumoto	2611-0259PUS1	2795

2292 7590 04/21/2010
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
BAUM, RONALD	
ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
04/21/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/588,803	MATSUMOTO, WATARU	
	Examiner	Art Unit	
	RONALD BAUM	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) *1-7* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8,11 and 12* is/are rejected.

7)☒ Claim(s) *9,10,13 and 14* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 August 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 09 August 2006.

2. Claims 1-14 are pending for examination, with claims 1-7 canceled.

3. Claims 8, 11 and 12 are rejected.

Claim Objections

4. Claims 8, 11 and 12 are objected to because of the following informalities: the phrase "capable of" is not a positive limitation but only requires the ability to so perform. It does not constitute a limitation in the patentable sense. In re Hutchison, 69 USPQ 138. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 8 recites the limitation "***the*** transmission data and ***error detection information***" in referring to "*error detection information* ". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 8, 11 and 12 are rejected under 35 U.S.C. 102(b) as being anticipated by Buttler, W., et al, ' Fast, efficient error reconciliation for quantum cryptography ', Univ. of Ca., Los Alamos National Laboratory, Los Alamos, NM 87545, (March 20, 2002), entire document, http://cdsweb.cern.ch/record/543746/files/0203096.pdf ("Buttler").

Prior Art's Broad Disclosure vs. Preferred Embodiments

As concerning the scope of applicability of cited references used in any art rejections below, as per MPEP § 2123, subsection R.5. Rejection Over Prior Art's Broad Disclosure Instead of Preferred Embodiments:

I. PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments. Merck & Co. v. Biocraft Laboratories, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), cert. denied, 493 U.S. 975 (1989). See also > Upsher-Smith Labs. v. Pamlab, LLC, 412 F.3d 1319, 1323, 75 USPQ2d 1213, 1215 (Fed. Cir. 2005)(reference disclosing optional inclusion of a particular component teaches compositions that both do and do not contain that component);< Celeritas Technologies Ltd. v. Rockwell International Corp., 150 F.3d 1354, 1361, 47 USPQ2d 1516, 1522-23 (Fed. Cir. 1998) (The court held that the prior art anticipated the claims even though it taught away from the claimed invention.). >See also MPEP § 2131.05 and § 2145, subsection X.D., which discuss prior art that teaches away from the claimed invention in the context of anticipation and obviousness, respectively.<

II. NONPREFERRED AND ALTERNATIVE EMBODIMENTS CONSTITUTE PRIOR ART

Disclosed examples and preferred embodiments do not constitute a teaching away from a broader disclosure or nonpreferred embodiments. In re Susi, 440 F.2d 442, 169 USPQ 423 (CCPA 1971). "A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use." In re Gurley, 27 F.3d 551, 554, 31 USPQ2d 1130, 1132 (Fed. Cir. 1994). Furthermore, "[t]he prior art's mere disclosure of more than one alternative does not constitute a teaching away from any of these alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed…." In re Fulton, 391 F.3d 1195, 1201, 73 USPQ2d 1141, 1146 (Fed. Cir. 2004).

Buttler *generally* teaches and suggests (i.e., Abstract, Sections I-VII in general) the limitations set forth in the claims below.

7. As per claim 8; "A quantum-key distributing method for a quantum cryptographic system including a transmission-side communication apparatus that transmits a random number sequence forming a basis of an encryption key in a predetermined quantum state on a quantum

communication path and a reception-side communication apparatus that measures a photon on the quantum communication path, the quantum-key distributing method comprising:

transmitting and receiving including

the reception-side communication apparatus maintaining

reception data with probability information obtained as a result of

measuring a light direction with a measuring device capable of

correctly identifying the light direction [*sections I, II, VI, VII, whereas in a classical QKD system (' transmitting and receiving including ... measuring a light direction with a measuring device ...') configured to utilize the error reconciliation protocol Winnow such that parity/hamming syndrome data sets, configured as matrix data structures with associated probability information, and transferred as part of the error reconciliation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.*]; and

the transmission-side communication apparatus maintaining

transmission data corresponding to

the reception data [*sections I, II, VI, VII, whereas in a classical QKD system configured to utilize the error reconciliation protocol Winnow such that parity/hamming syndrome data sets, configured as matrix data structures with associated probability information and communications data, and transferred as part of the error reconciliation,*

clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

information notifying including

the transmission-side communication apparatus notifying,

via a public communication path,

the reception-side communication apparatus of

error correction information generated

based on a parity check matrix,

of which elements are "0" or "1", and

the transmission data and error detection information

generated based on

a cyclic code for detecting an error and

the transmission data [*sections II-IV, whereas in a classical QKD system configured to utilize the error reconciliation protocol Winnow ('... transmission-side ... notifying ... public ... path ... reception-side ...') such that parity/hamming syndrome data sets ('... cyclic code for detecting an error ...'), configured as matrix data structures with associated probability information, and transferred as part of the error reconciliation ('... error correction ... based on a parity check matrix ... elements are "0" or "1" ... '), clearly encompasses the claimed limitations as broadly interpreted by the examiner.*];

transmission-data estimating including

the reception-side communication apparatus

estimating the transmission data based on

a same parity check matrix as that of

the transmission-side communication apparatus,

the reception data with probability information,

the error correction information, and

the error detection information [*sections I-IV, VII whereas in a classical QKD system configured to utilize the error reconciliation protocol Winnow ('... reception-side ... estimating the transmission data ... same parity check matrix ... transmission-side ...') such that parity/hamming syndrome data sets, configured as matrix data structures with associated probability information ('... reception data with probability information ...'), and transferred as part of the error reconciliation ('... same parity check matrix ... error correction ... error detection ... '), clearly encompasses the claimed limitations as broadly interpreted by the examiner.*]; and

encryption-key generating including

the transmission-side communication apparatus and

the reception-side communication apparatus

discarding a part of the transmission data according to

an amount of opened information and

generating an encryption key

using rest of the transmission data [*sections I-IV, VII whereas in a classical QKD system configured to utilize the error reconciliation protocol Winnow such that parity/hamming syndrome data sets, configured as matrix data structures with associated probability information, and transferred as part of the error reconciliation, prior to the actual key generation ('... encryption-key generating ... using rest of the transmission data '), clearly encompasses the claimed limitations as broadly interpreted by the examiner.*].".

As per claim 11, this claim is the system transmit side claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection; "A communication apparatus that constitutes a quantum cryptographic system in which apparatuses share an encryption key through quantum key distribution, and transmits a random number sequence forming a basis of the encryption key to a quantum communication path in a predetermined quantum state, the communication apparatus comprising:

an information notifying unit that notifies, via a public communication path, the other apparatus of error correction information and error detection information, the error correction information being generated based on transmission data corresponding to reception data of the other apparatus obtained as a result of measuring a light direction with a measuring device capable of correctly identifying the light direction and a same parity check matrix as that of the other apparatus, the error detection information being generated based on the transmission data and a cyclic code for detecting an error; and

an encryption-key generating unit that discards a part of the transmission data according to an amount of opened information, and generates an encryption key using rest of the transmission data.".

As per claim 12, this claim is the system receive side claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection; "A communication apparatus that constitutes a quantum cryptographic system in which apparatuses share an encryption key through quantum key distribution, and measures a photons, which is a random number sequence forming a basis of the encryption key, on a quantum communication path, the communication apparatus comprising:

a transmission-data estimating unit

that estimates original transmission data based on

a parity check matrix identical to that of

other apparatus that shares the encryption key,

reception data with probability information obtained by

measuring a light direction with a measuring device

capable of correctly identifying the light direction, and

error correction information and error detection information

received from other apparatus

via a public communication path; and

an encryption-key generating unit

that discards a part of the transmission data according to

an amount of opened information, and

generates an encryption key

using rest of the transmission data.".

Allowable Subject Matter

8. Claims 9, 10, 13 and 14 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

9. Claim 9 ***additionally*** recites the limitation that; "The quantum-key distributing method according to claim 8, wherein the transmission-data estimating includes

setting a prior value

corresponding to an element "1" in the parity check matrix

as initial setting;

executing, row by row, a first process of updating, an external value

corresponding to the element "1" in the parity check matrix

using a prior value

corresponding to another element "1" in an identical row and

the probability information according to

the error correction information;

executing, column by column, a second process of updating the prior value

corresponding to the element "1" in the parity check matrix

using an external value after the update

corresponding to another element "1" in an identical column;

calculating posterior probability based on

the probability information and the prior value after the update and

judging a temporary estimated word

from the posterior probability; and

detecting,

when the temporary estimated word satisfies a predetermined condition

established between

the temporary estimated word and

the parity check matrix,

an error for the temporary word

using the error detection information,

judging, if there is no error,

that the temporary estimated word

is original transmission data, and

repeatedly executing,

when the temporary estimated word

does not satisfy the predetermined condition,

the first process,

the second process, and

a process of judging the temporary estimated word

using the value after the update

until the condition is satisfied.".

As per claim 13, this claim is the system claim for the method claim 9 above, and is objected to for the same reasons provided for the claim 9 rejection; "The communication apparatus according to claim 12, wherein the transmission-data estimating unit performs

setting a prior value corresponding to an element "1" in the parity check matrix as initial setting,

executing, row by row, a first process of updating, an external value corresponding to the element "1" in the parity check matrix using a prior value corresponding to another element "1" in an identical row and the probability information according to the error correction information,

executing, column by column, a second process of updating the prior value corresponding to the element "1" in the parity check matrix using an external value after the update corresponding to another element "1" in an identical column,

calculating posterior probability based on the probability information and the prior value after the update and judging a temporary estimated word from the posterior probability, and

detecting, when the temporary estimated word satisfies a predetermined condition established between the temporary estimated word and the parity check matrix, an error for the temporary word using the error detection information,

judging, if there is no error, that the temporary estimated word is original transmission data, and

repeatedly executing, when the temporary estimated word does not satisfy the predetermined condition, the first process, the second process, and a process of judging the temporary estimated word using the value after the update until the condition is satisfied.".

10. Claim 10 ***additionally*** recites the limitation that; "The quantum-key distributing method according to claim 9, wherein the transmission-data estimating includes

comparing

the error detection information and

estimated error detection information

generated using the temporary estimated word,

judging,

if

the error detection information and

the estimated error detection information

coincide with each other,

that there is no error in

the temporary estimated word, and

judging,

if

the error detection information and

the estimated error detection information

do not coincide with each other,

that there is an error in

the temporary estimated word.".

As per claim 14, this claim is the system claim for the method claim 10 above, and is objected to for the same reasons provided for the claim 10 rejection; "The communication apparatus according to claim 13, wherein the transmission-data estimating unit performs

comparing the error detection information and estimated error detection information generated using the temporary estimated word,

judging, if the error detection information and the estimated error detection information coincide with each other, that there is no error in the temporary estimated word, and

judging, if the error detection information and the estimated error detection information do not coincide with each other, that there is an error in the temporary estimated word.".

Conclusion

11. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad, can be reached at (571) 272-7884. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

/R. B./

Examiner, Art Unit 2439

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439